REMARKS

In the Office Action dated September 1, 2005, claims 13-19, 21, 22, 25, and 26 were rejected under 35 U.S.C. § 103 over U.S. Patent No. 5,204,663 (Lee) in view of U.S. Patent No. 6,057,764 (Williams); and claims 23 and 24 were rejected under § 103 over Lee in view of Williams and U.S. Patent No. 6,624,739 (Stobbe).

RESTRICTION REQUIREMENT

A Petition from Requirement for Restriction Under 37 C.F.R. § 1.144 was filed on November 3, 2005. A copy of the Petition is attached (Exhibit A) for the convenience of the Examiner. The substance of the Petition is hereby incorporated into the present reply to challenge the restriction requirement.

REJECTIONS UNDER 35 U.S.C. § 103

It is respectfully submitted that a *prima facie* case of obviousness has not been established with respect to claim 13 over Lee and Williams, for at least the following reasons: (1) there existed no motivation or suggestion to combine reference teachings; and (2) the references when combined do not teach or suggest *all* elements of the claim. M.P.E.P. § 2143 (8th ed., Rev. 3), at 2100-135.

Point (2) is addressed first. The Office Action cited column 3, line 42-column 4, line 3 of Lee as teaching the first assigning act of claim 13, which recites "assigning database information a plurality of clearance levels." The cited passage in columns 3 and 4 of Lee refers to smart cards of different categories, including: installer cards for use by workmen to install an acceptor and an opening mechanism for an access control system on a door; a setup card to set up initial access codes; a services card to provide access to a room by an authorized person other than a customer; and a customer card to provide access to customers to a particular access-controlled area. There is no teaching or suggestion in this cited passage of *assigning database information* a plurality of clearance levels, as recited in claim 13. This is a first point of error made in the Office Action.

A second point of error made by the Office Action is the citation of column 5, lines 15-18, of Lee as teaching the task of identifying a lowest clearance level assigned to the smart badges within a boundary. The cited passage of Lee refers to supervisors having access to multiple floors, and a security officer having access to every door. The cited passage also states that the method of assigning codes is fully programmable by a system manager. There is absolutely no indication or suggestion whatsoever in the passage of Lee of identifying a lowest clearance level assigned to smart badges (note the plural sense of "smart badges") within a *boundary*. In fact, such an identification is impossible using the system described by Lee. In the Lee system, a card acceptor 100 (see Figs. 1 and 4 of Lee) has an opening 101 (see Fig. 4 of Lee) through which *a* smart card is entered. Lee, 6:64-68; 8:16-19, 36-37. The single smart card entered into the card acceptor of Lee *conductively engages* the acceptor. Lee, 6:67-68. In fact, the card acceptor 100 has an electro-mechanical device to *physically receive* the smart card and *conductively engage the I/O contact pads* of the smart card with the card acceptor 100. Lee, 8:16-19. The card acceptor 100 has a microswitch 102 that is spring loaded near the opening 101 of the card acceptor 100, and a contact mechanism that conductively engages the I/O contact

pads of the smart card with the card acceptor 100 when the card is fully entered into the opening 101. Lee, 8:36-42. Thus, it is clear that the card acceptor described in Lee can read only one card at a time, and in fact, the card acceptor of Lee requires that this card must be entered into an opening of the card acceptor. Therefore, it is physically impossible for the card acceptor 100 of Lee to identify a lowest clearance level assigned to *plural* smart badges within a boundary.

A third point of error made by the Office Action is the citation of column 5, lines 1-67, of Lee as teaching the providing task of claim 13, which recites "providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level." The cited passage in column 5 of Lee refers to the acceptor (which receives, in an opening, a smart card to read the smart card) managing multiple, differing levels of security for guest access, emergency access, security access, inspector access, supervisor access, and housekeeper access to a hotel room. Different codes are assigned for each level of security. The smart cards are then used by employees or hotel guests to enter different rooms of a hotel. Providing a smart card that behaves as a key to enter different rooms or areas of a hotel or other building, as taught by Lee, is not the same as providing access to a *sub-set of database information* having a clearance level no higher than the lowest identified clearance level. In Lee, smart cards are used to enable or disable entry into a room, not to provide access to a sub-set of database information.

Based on at least these three points of clear error made by the Office Action, a *prima facie* case of obviousness has not been established with respect to claim 13 over the asserted combination of Lee and Williams. Because Lee does not disclose at least three elements of claim 13 that the Office Action contended was disclosed by Lee, it would be impossible for the hypothetical combination of Lee and Williams to teach or suggest all elements of claim 13. A *prima facie* case of obviousness has not been established for at least this reason.

Moreover, the Office Action conceded that "Lee does not explicitly teach wireless beacon." 9/1/2005 Office Action at 5. This concession necessarily means that Lee does not disclose using a wireless beacon to detect which smart badges are located within a predetermined physical boundary.

The Office Action cited Williams as disclosing the feature of claim 1 that was conceded as not being disclosed by Lee. However, Applicant respectfully submits that the proposed combination of Lee and Williams is improper since no motivation or suggestion existed to combine the teachings of Lee and Williams to achieve the claimed invention.

As discussed above, Lee teaches an acceptor to receive, in an opening, a single smart card to determine whether a user can open a door to gain access to an access-controlled area, such as a hotel room. On the other hand, Williams teaches motion detectors associated with transceivers that are able to determine if an authorized user is in a secure space such that an alarm is not sounded in response to detecting presence of an authorized user. This teaching of Williams does not provide the requisite suggestion or motivation to modify Lee's acceptor/smart card mechanism, which controls access to a room, to achieve the method of claim 1.

In fact, there would have been absolutely no reason whatsoever to incorporate the teachings of Williams into the system of Lee. It is well-established law that "[t]he mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." *In re Gordon,* 733 F.2d 900, 902, 221 U.S.P.Q. 1125 (Fed. Cir. 1984). Here, Lee clearly teaches that a smart card has to be physically entered into an opening of a card acceptor to achieve physical engagement for the purpose of gaining access to a room. There is no indication of any desirability of using any type of wireless mechanism to detect smart badges located within a predefined physical boundary. Such a mechanism would in fact violate the security concerns being addressed by Lee. It would be undesirable for a room entry card acceptor used by Lee to detect smart badges within a boundary, such as a hallway of a hotel, since providing such a feature would allow for easier unauthorized entry. Therefore, it is respectfully submitted that because no motivation or suggestion existed to combine the teachings of Lee and Williams to achieve the claimed invention, a *prima facie* case of obviousness has not been established with respect to claim 13.

Independent claim 21 is allowable for similar reasons as claim 13.

Dependent claims are allowable for at least the same reasons as corresponding independent claims. Moreover, in view of the defective obviousness rejection of base claims over the asserted combination of Lee and Williams, it is respectfully submitted that the obviousness rejection of dependent claims 23 and 24 over Lee, Williams, and Stobbe is also defective.

Dependent claim 14 (which depends from claim 13) is further allowable since the hypothetical combination of Lee and Williams does not disclose or suggest the additional elements of claim 14. The Office Action stated that column 2, lines 3-10, of Lee discloses the task of defining those smart badges within the boundary as a set of visible smart badges. 9/1/2005 Office Action at 6. The cited passage of Lee refers to providing a key (smart card) with a sufficient memory capacity to carry access information required for entry to an access-controlled area, such as a hotel room. There is absolutely no suggestion anywhere here of defining smart badges *within a boundary* as a set of *visible smart badges*. The Office Action also mistakenly cites column 2, lines 10-14, of Lee as disclosing the task of updating the set of visible smart badges in response to a change in smart badge visibility status. The cited passage of Lee refers to changing an access code as often as required by a system manager, and the provision of several access codes corresponding to different levels of access. This passage of Lee clearly does not disclose updating a set of visible smart badges in response to a change in smart badge visibility status. Thus, claim 14 is further allowable for this additional reason.

Claim 15 (which depends from claim 14) is further allowable since the Office Action incorrectly noted that Lee teaches recalculating the lowest clearance level in response to the change in smart badge visibility status. The Office Action cited column 5, lines 62-67, of Lee as teaching this feature. However, this passage of Lee describes that for extremely sensitive areas, the system can be programmed not to admit a person who has logged into the facility, but has not logged out, to prevent more than one person from using a card to gain admittance to a secure facility. There is absolutely no suggestion whatsoever in this passage of Lee of recalculating the lowest clearance level in response to a change in smart badge visibility status.

Claim 16 (which depends from claim 13) is further allowable in view of the Office Action incorrectly stating that Williams teaches providing access to database information to smart badge wearers assigned to the smart badges. Specifically, the Office Action cited column 6, lines 2-9, of Williams as teaching this feature. The cited passage of Williams refers to a computer searching among authorized identification numbers for a particular space to determine if the identification number in question (associated with a badge worn by a badge wearer) has a tag indicating authority to be within the particular space of the potential alarm. In other words, this passage merely refers to the determination made by a computer of whether a badge wearer is in fact authorized to be in a particular space so that no alarm will be sounded if that were the

case. There is absolutely no suggestion here of providing access to *database information* to smart badge wearers assigned to smart badges.

Claim 17 (which depends from claim 14) is further allowable because the Office Action incorrectly noted that Lee teaches preventing access to the database when the smart badge visibility status is set to invisible for a predetermined timeout. Specifically, the Office Action cited column 11, lines 22-43, of Lee as disclosing this feature. This passage of Lee describes enabling access to a room for a customer card, where the check-in and check-out times (associated with check-in and check-out of a hotel room) are read to determine whether access is to be provided to a hotel room. The passage also refers to examining the code representing the security level assigned to the card to check whether the security level code is greater than the security level code that is prestored. Neither of these tasks even remotely suggests preventing access to a *database* when the smart badge *visibility status* is set to *invisible* for a predetermined timeout. Preventing access to a room is not the same as preventing access to a database.

Claim 18, which depends from claim 13, is further allowable because the Office Action incorrectly stated that Williams teaches defining a badge removal confidence level indicating whether each smart badge has been continuously worn by corresponding assigned smart badge wearers. The Office Action cited column 6, lines 2-18, of Williams as disclosing this feature. This passage of Williams refers to determining whether an added indication number associated with a badge is authorized to be within the particular space. The cited passage also refers to a badge receiving a cryptographic code upon entry of a building that is concomitant with visual recognition of the employee. However, there is absolutely no indication whatsoever of defining a badge removal confidence level indicating whether each smart badge has been *continuously worn* by corresponding assigned smart badge wearers.

Claim 19 (which depends from claim 13) is further allowable because the Office Action incorrectly stated that Lee discloses de-authenticating and erasing all data stored on a smart badge whose expiration period has been exceeded. Specifically, the Office Action cited column 4, lines 56-64, of Lee as disclosing this feature. The cited passage of Lee refers to retaining a primary access code in the *acceptor* until a new guest uses the room, at which time the primary access code in the new guest's card will replace the acceptor's existing access code. What this passage is referring to is the replacement of a code in the *acceptor*. There is no suggestion here whatsoever of de-authenticating and erasing all data stored on a *smart badge.*

Claim 25 (which depends from claim 21) is allowable for similar reasons as claim 15.

In view of the foregoing, allowance of all claims is respectfully requested. The Commissioner is authorized to charge any additional fees and/or credit any overpayment to Deposit Account No. 08-2025 (10005248-1).

Respectfully submitted,

Date: Nov. 30, 2005

Dan C. Hu
Registration No. 40,025
TROP, PRUNER & HU, P.C.
8554 Katy Freeway, Suite 100
Houston, TX 77024
Telephone: (713) 468-8880
Facsimile: (713) 468-8883